UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/721,942	11/27/2000	Ulf Mattsson	65747(53142)	4284

21874 7590 11/29/2006

EDWARDS & ANGELL, LLP
P.O. BOX 55874
BOSTON, MA 02205

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 11/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/721,942	MATTSSON ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 August 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 08/30/06. Claims 1, 7, 9 and 11 have been amended; claims 12-15 have been added.

Response to Arguments

2. Applicant's arguments, see page 8, first full paragraph, with respect to claim 1 have been considered but are not persuasive. Applicant's amendments have necessitated a new search and new grounds of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-3 and 6-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wessman (7,111,005) in view of Date ("An Introduction to Database Systems"). Wessman discloses a method and system for automatic and transparent database encryption (Abstract).

Regarding claims 1-2 and 7-15, Wessman discloses a method and system for encrypting a particular column in a database comprising: reading an existing data element (i.e., national ID or NID) from a particular column (i.e., column 226 of table 218), the data element including a first character string; encrypting the first character string into a second character string (encrypted NID); and storing the second character string in the particular column (col. 4, lines 22-29; figure 5 and corresponding text). Wessman does not explicitly disclose forming a restricting character set on the data type of the data element and each character in the second character string being selected from the restricting character set. However, these features are deemed to be inherent to the Wessman method since each data column of a data table in a database system is associated with a particular data type and that the database system only accepts a data element to be stored in a particular column if the data type of the data element matches the associated data type of that particular column. Inherently, Wessman's first character string and second character string must be of the same data type which defines a restricting character set.

Wessman does not disclose reading information identifying the data type of the particular column from a location in the database but outside of the particular column. Date discloses reading metadata including information identifying the data type of a column of a table and the

metadata being stored within the database but outside of the column (figure 2.4, page 45; Section 3.6, pages 69-70; Section 8.3, pages 252-253). It would have been obvious to one of ordinary in the art at the time the invention was made to modify the Wessman method to read information identifying the data type of the particular column from the metadata, as taught by Date. The metadata contains detailed information of various objects in a database and is readily available.

Regarding claims 3 and 6, Wessman further discloses using DES algorithm (col. 4, lines 46-49). Inherently, a plaintext and the corresponding ciphertext generated by DES algorithm have the same number of characters.

5. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wessman in view of Date as applied to claim 1 above, and further in view of Schneier ("Applied Cryptography"). Wessman does not disclose converting each character of said first character string to an index value and adding a varying value to each index value before encryption. Schneier discloses an encryption method called one-time pad including the steps of converting each character to an index value and adding a varying value to each index value before encryption (Section 1.5, page 15). It would have been obvious to one of ordinary skill in the ad at the time the invention was made to

modify the combined method of Wessman and Date to include the steps of converting each character of said first character string to an index value and adding a varying value to each index value before encryption, as taught by Schneier. The one-time pad is a perfect encryption scheme.

6. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wessman in view of Date and Schneier as applied to claim 4 above, and further in view of Marshall et al. (4,866,707).

Wessman, Date and Schneier do not disclose adding adjacent index values pairwise from the left to the right using said initial value when adding the leftmost character. Schneier, in Section 9.3, discloses a cipher block chaining (CBC) mode in which adjacent blocks are XORed pairwise from the left to the right using an initialization vector with the leftmost unit (page 194, fig. 9.3 and "Prevent this by encrypting ... use some random bits from someplace"); the teaching of Schneier reads on the adding step of the claim. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Wessman, Date and Schneier (Section 1.5) to include the step of adding adjacent index values pairwise from the left to the right using said initial value when adding the leftmost character, as taught by Schneier (Section 9.3). The motivation for doing so would have been that the ciphertext block is dependent not just on

the plaintext block that generated it but on all the previous plaintext blocks (page 193).

Wessman, Date and Schneier do not disclose creating an initial value by hashing an encryption key. Marshall discloses a CBC encryption technique including the step of creating an initialization vector by encrypting a message key (col. 9, lines 13-19); the teaching of Marshall reads on the creating step of the claim. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify combined method of Wessman, Date and Schneier to include the step of creating an initial value by hashing the encryption key, as taught by Marshall. The motivation for doing so would have been that the same message being sent a second time would be encrypted under a different key, so an outsider would not be able to gain much assistance from the repetition in trying to breach the encryption (col. 9, lines 27-33).

7. Claims 1-3 and 7-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Morar et al (6,678,822) in view of Date.

Regarding claims 1, 7 and 12-15, Morar discloses a method for encrypting restricted information in an information container such as a document or a database (col. 4, lines 7-12), the method comprising: reading a data type of a data element; reading a data element including a first

character string from the information container; forming a restricting character set; and encrypting said first character string into a second character string, each character in said second character string being selected from said restricting character set (col. 1, lines 36-46; col. 5, lines 34-56; col. 8, line 55 – col. 9, line 14; col. 11, lines 37-58). Morar uses a document as an information container in the specification for illustration of his method, and, therefore, does not explicitly disclose a column of a database and a data type associated the column; however, these features are deemed to be inherent to a database.

Morar discloses reading information identifying the data type of a data element by analyzing the element itself. Morar does not disclose reading information identifying the data type of the particular column from a location in the database but outside of the particular column. Date discloses reading metadata including information identifying the data type of a column of a table and the metadata being stored within the database but outside of the column (figure 2.4, page 45; Section 3.6, pages 69-70; Section 8.3, pages 252-253). It would have been obvious to one of ordinary in the art at the time the invention was made to modify the Morar method to read information identifying the data type of the particular column from the metadata, as taught by Date. The metadata contains detailed information of various objects in a database and is readily available.

Regarding claim 2, Morar further discloses processing character-based information (col. 9, lines 9-14; col. 11, lines 53-58). Inherently, characters of a character set are arranged in a pattern for a data type so that a data type such as number can be recognized.

Regarding claim 3, Morar further discloses that the number of characters in the second character string is equal to the number of characters in the first character string (col. 9, lines 9-14).

Regarding claims 8-11, Morar further discloses that the encryption is performed on a working copy of a database and that the second character string is stored in the data element replacing the first character string (col. 8, line 41 – col. 9, line 14).

8. Claims 4 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Morar in view of Date as applied to claim 1 above, and further in view of Schneier ("Applied Cryptography").

Regarding claim 4, Morar further discloses replacing characters of a data element with random characters of the same data type (col. 9, lines 9-14; col. 11, lines 53-58). Inherently, each character of the first character string is assigned an index value. However, Morar does not disclose adding a varying value to each index value before encryption. Schneier discloses an encryption method called one-time pad including the steps of converting

each character to an index value and adding a varying value to each index value before encryption (Section 1.5, page 15). It would have been obvious to one of ordinary skill in the ad at the time the invention was made to modify the combined method of Morar and Date to include the step of adding a varying value to each index value before encryption, as taught by Schneier. The one-time pad is a perfect encryption scheme.

Regarding claim 6, Morar does not disclose using the DES algorithm in stream cipher mode. Schneier discloses using the DES algorithm in CFB mode of operation, which meets the limitation of DES algorithm in stream cipher mode (Section 12.2, page 277, see Modes of DES). It would have been obvious to one of ordinary skill in the ad at the time the invention was made to modify the combined method of Morar and Date to use the DES algorithm in stream cipher mode. The motivation for doing so would have been that the 8-bit CFB is generally the mode of choice for encrypting stream of characters when each character has to be treated individually (Section 9.11, page 210).

9. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Morar in view of Date and Schneier as applied to claim 4 above, and further in view of Marshall et al. (4,866,707).

Morar, Date and Schneier (Section 1.5) do not disclose adding adjacent index values pairwise from the left to the right using said initial value when adding the leftmost character. Schneier, in Section 9.3, discloses a cipher block chaining (CBC) mode in which adjacent blocks are XORed pairwise from the left to the right using an initialization vector with the leftmost unit (page 194, fig. 9.3 and "Prevent this by encrypting ... use some random bits from someplace"); the teaching of Schneier reads on the adding step of the claim. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Morar, Date and Schneier (Section 1.5) to include the step of adding adjacent index values pairwise from the left to the right using said initial value when adding the leftmost character, as taught by Schneier (Section 9.3). The motivation for doing so would have been that the ciphertext block is dependent not just on the plaintext block that generated it but on all the previous plaintext blocks (page 193).

Morar, Date and Schneier do not disclose creating an initial value by hashing an encryption key. Marshall discloses a CBC encryption technique including the step of creating an initialization vector by encrypting a message key (col. 9, lines 13-19); the teaching of Marshall reads on the creating step of the claim. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify combined

method of Morar, Date and Schneier to include the step of creating an initial value by hashing the encryption key, as taught by Marshall. The motivation for doing so would have been that the same message being sent a second time would be encrypted under a different key, so an outsider would not be able to gain much assistance from the repetition in trying to breach the encryption (col. 9, lines 27-33).

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Oracle8i Supplied PL/SQL Packages Reference Release 2 (8.1.6) - DBMS_OBFUSCATION_TOOLKIT

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-

MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MP

Minh Dinh
Examiner
Art Unit 2132

KAMBIZ ZAND
PRIMARY EXAMINER

MD
11/26/06